[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06K 19/07
G06F 9/06 G06F 12/00
G06F 13/00

[12] 发明专利申请公开说明书

[21] 申请号 02126542.9

[43] 公开日 2004 年 1 月 28 日

[11] 公开号 CN 1471050A

[22] 申请日 2002.7.23 [21] 申请号 02126542.9

[71] 申请人 深圳市明华澳汉科技有限公司
地址 518028 广东省深圳市华强北上步工业区 11 栋东三楼
[72] 发明人 韩业勤

[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 汪惠民

权利要求书 14 页 说明书 25 页 附图 7 页

[54] 发明名称 集成电路卡的数据操作方法及装置

[57] 摘要

本发明提供了一种集成电路卡的数据操作方法及装置，应用在集成电路卡上，可做到对人、对卡、对系统的三方的合法性认证，保证了卡的安全性。

ISSN1008-4274

1、一种集成电路卡的数据操作方法，包括以下步骤：

初始化步骤，初始化集成电路卡的工作区，集成电路卡的工作区主要用于临时工作数据的暂存；

计算步骤，计算存储器中的系统控制信息的完整性，存储器主要存储应用程序和数据，系统控制信息包括但不限于起始地址、终止地址、卡片状态、操作系统的版本号、程序控制字节、CRC 校验；

完整性判断步骤，判断系统控制信息的完整性；

程序控制步骤，对系统控制信息中的程序控制字节进行判断，决定或者执行存储器中的应用程序，或者准备相应协议的复位信息；

复位响应判断步骤，判断是否建立复位响应文件；

取响应数据步骤，取复位响应文件中的复位响应数据；

发送步骤，发送复位响应数据；

恢复步骤，恢复备份数据；

协议判断步骤，判断通讯协议是否为 T=0；

传输步骤，卡接受由接口设备传输过来的命令头，命令头包括但不限于指令类型、指令代码、参数；

指令判断步骤，判断是否特殊指令；

状态判断步骤，判断卡片状态是否正确；

清标志步骤，清工作标志；

协议处理步骤，如果是 T=0 协议，则返回指令代码，发送应答数据；如果是 T=1 协议，则延时，设置节点地址的值和设置协议控制字节的值，发送应答数据；

协议设置步骤，判断通讯协议标志，设置通讯协议类型；

返回复位响应判断步骤。

2、根据权利要求 1 所述的集成电路卡的数据操作方法，其所述的完整性判断步骤，如果不完整，则锁卡并更新存储器中的系统控制信息，然后执行程序控制步骤；

3、根据权利要求 1 所述的集成电路卡的数据操作方法，其所述的程序控制步骤中执行存储器中的应用程序一般为集成电路卡使用者自己设定的加密程序。

4、根据权利要求 1 所述的集成电路卡的数据操作方法，其所述的复位响应判断步骤，如果不建立复位响应文件，则将复位响应设置为芯片的序列号，然后执行发送步骤。

5、根据权利要求 1 所述的集成电路卡的数据操作方法，其所述的协议判断步骤，如果通讯协议为 T=1，则执行如下步骤：

接收地址步骤，接收节点地址；

第一接收判断步骤，判断接收是否正确；

第一超时判断步骤，判断是否超时；

接收控制字节步骤，接收协议控制字节；

第二接收判断步骤，判断接收是否正确；

第二超时判断步骤，判断是否超时；

接收长度步骤，接收数据域的长度；

第三接收判断步骤，判断接收是否正确；

第三超时判断步骤，判断是否超时；

接收数据步骤，接收数据；

接收校验步骤，接收校验和；

校验判断步骤，判断校验和是否正确；

然后返回指令判断步骤；

6、根据权利要求 5 所述的集成电路卡的数据操作方法，其所述的第一接收判断步骤，如果接收不正确，则置错误标志，然后返回接收控制步骤。

7、根据权利要求 5 所述的集成电路卡的数据操作方法，其所述的第二接收判断步骤，如果接收不正确，则置错误标志，然后返回接收长度步骤。

8、根据权利要求 5 所述的集成电路卡的数据操作方法，其所述的第三接收判断步骤，如果接收不正确，则置错误标志，然后返回接收数据步骤。

9、根据权利要求 5 所述的集成电路卡的数据操作方法，其所述的校验判断步骤，如果校验和不正确，则置错误标志，然后返回接收指令判断步骤。

10、根据权利要求 1 所述的集成电路卡的数据操作方法，其所述的指令判断步骤，如果不是特殊指令，则执行如下步骤：

查找步骤，查找命令类型表；

查找判断步骤，判断查找是否成功；

取命令表步骤，根据程序控制字节判断命令表的存放位置，相应的取 EEPROM 或 ROM 中的命令表；

查找命令判断步骤，判断查找命令是否成功；

命令类型判断步骤，判断命令类型是否成功；

命令处理步骤，如果是 T=0 的协议，则返回指令代码，并判断是否接收数据，是则接收数据，否则直接执行命令判断步骤；

命令判断步骤，判断是否满足执行条件；

执行命令步骤，执行相应命令；

返回复位响应判断步骤。

11、根据权利要求 10 所述的集成电路卡的数据操作方法，其所述的查找判断步骤，如果查找不成功，则置错误代码，并返回复位响应判断步骤。

12、根据权利要求 10 所述的集成电路卡的数据操作方法，其所述的查找命令判断步骤，如果查找不成功，则置错误代码，并返回复位响应判断步骤。

13、根据权利要求 10 所述的集成电路卡的数据操作方法，其所述的命令类型判断步骤，如果不成功，则置错误代码，并返回复位响应判断步骤。

14、根据权利要求 1 所述的集成电路卡的数据操作方法，其文件结构包括：

主控文件（Master,MF），主控文件是整个文件系统的根，可看作根目录，每个集成电路卡有且只有一个主控文件，它是在卡的个人化过程中首先被建立起来的，在卡的整个生命周期内一直存在并保持有效，可存储卡的公共住处并为各种应用服务；由个人化建立起来的主控文件包括文件控制参数以及文件安全属性等信息；在物理上，主控文件占有存储空间包括 MF 文件头的大小以及 MF 所管理的 EF 和 DF 的存储空间；

专用文件(Dedicated File,DF)，在 MF 下针对不同的应用建立起来的一种文件，是位于 MF 之下的含有 EF 的一种文件结构（可看作文件目录），它存储了某个应用的全部数据以及与应用操作相关的安全数据；

DF 由创立文件命令建立，它的大小在建立后没有被确定，随其下建文件的空间大小而改变，对 DF 的建立操作由 MF 的安全属性控制；

在 DF 下面不可再建立 DF，只能建立 EF；

为了保证各个 DF 的相互独立，只能从文件系统的 MF 层次选择一个 DF，对 DF 下的数据进行的操作由各当前系统的安全状态控制；

基本文件（Elementary File,EF），基本文件存储了各种应用的数据和管理信息，它存在于 MF 或 DF 下；

整个文件系统的空间在 MF、DF 和 EF 建立时被分配和确定，以后在物理上不会发生变化，当访问 EF 时，必须先选择相应的 MF 或 DF；

可以从文件系统的任何位置选择 MF。

15、根据权利要求 14 所述的集成电路卡的数据操作方法，其所述的基本文件从存储内容上分为两类：安全基本文件和工作基本文件；

安全基本文件（Secret Elementary File,SEF）的内容包括用于识别和与加密有关的保密数据（个人识别码、密钥等），卡将利用这些数据进行安全管理，SEF 要在 MF 或 DF 建立后，才能建立，安全基本文件的内容不可被读出，但可使用专门的方法来写入或修改，

在 MF 和每个 DF 下只能建立 1 个安全基本文件；

工作基本文件（Working Elementary File, WEF）包含了应用的实际数据，其内容不被卡解释，在符合 WEF 的读、修改安全属性时，可对其内容进行读取、修改，工作文件的个数和大小受到 MF 或 DF 所拥有空间的限制。

16、根据权利要求 14 所述的集成电路卡的数据操作方法，其所述的基本文件的结构包括：

二进制结构，二进制文件为一个数据单元序列，数据以字节为单位进行读写，其中的数据结构则由应用解释；

线性定长记录文件结构，这种结构以固定的长度来处理每条记录；通过逻辑上连续的记录号，可访问这类记录，记录号的范围是 1 至 254，记录长度最长为 249 字节；每次访问只对一条记录进行操作，而且必须严格遵守记录长度的规定，

线性定长记录文件结构，在这类结构中，每条记录的长度可以各不相同；仍然是以记录号来访问各条记录。在读记录时，操作与线性定长记录的相同，写记录时可以与原记录长度不同，但不能超过原记录长度；添加记录时，记录的长度不能超过最大记录长度（249 字节）的规定；

循环定长记录文件结构，一类特殊的定长记录文件结构；在逻辑上，这类文件可看作一个环形记录队列，记录按照先进先出的原则存储；添加记录时，最新一次写入的记录的记录为 1，上一次写入的记录的记录号为 2，依次类推；记录的个数与预留的记录的记录空间大小以及记录的长度相关，记录个数=记录空间大小整除记录

长度；

此外还有一些只能特殊使用的文件类型，如 ATR、钱包文件、存折文件、密钥文件等，但其文件结构也不超出以上四种文件的类型。

17、根据权利要求 14 所述的集成电路卡的数据操作方法，其所述的文件组织如下：

主控文件含有但不限于下列数据：文件名，文件标识符，所属文件的管理权限，所属专用文件的链表，所属基本文件的链表，卡片的可用空间地址，卡片的状态；

专用文件含有不限于下列数据：文件名，文件标识符，所属文件的管理权限，所属专用文件的链表，下一个专用文件的链表，所属基本文件的链表，专用文件的状态；

基本文件含有但不限于下列数据：文件名，文件标识符，基本文件的安全条件，基本文件的状态，文件长度或记录数和记录长度，记录指针；

各文件间以指针的形式实现相互间的联系。

18、一种集成电路卡的数据操作装置，其特征在于：包括以下装置：

初始化装置，初始化集成电路卡的工作区，集成电路卡的工作区主要用于临时工作数据的暂存；

计算装置，计算存储器中的系统控制信息的完整性，存储器主要存储应用程序和数据，系统控制信息包括但不限于起始地址、终止地址、卡片状态、操作系统的版本号、程序控制字节、CRC 校验；

完整性判断装置，判断系统控制信息的完整性；

程序控制装置，对系统控制信息中的程序控制字节进行判断，决定或者执行存储器中的应用程序，或者准备相应协议的复位信息；

复位响应判断装置，判断是否建立复位响应文件；

取响应数据装置，取复位响应文件中的复位响应数据；

发送装置，发送复位响应数据；

恢复装置，恢复备份数据；

协议判断装置，判断通讯协议是否为 T=0；

传输装置，卡接受由接口设备传输过来的命令头，命令头包括但不限于指令类型、指令代码、参数；

指令判断装置，判断是否特殊指令；

状态判断装置，判断卡片状态是否正确；

清标志装置，清工作标志；

协议处理装置，如果是 T=0 协议，则返回指令代码，发送应答数据；如果是 T=1 协议，则延时，设置节点地址的值和设置协议控制字节的值，发送应答数据；

协议设置装置，判断通讯协议标志，设置通讯协议类型；

返回复位响应判断装置。

19、根据权利要求 18 所述的集成电路卡的数据操作装置，其特征在于所述的完整性判断装置，如果不完整，则锁卡并更新存储器中的系统控制信息，然后执行程序控制装置；

20、根据权利要求 18 所述的集成电路卡的数据操作装置，其特征在于所述的程序控制装置中执行存储器中的应用程序一般为集成

电路卡使用者自己设定的加密程序。

21、根据权利要求 18 所述的集成电路卡的数据操作装置，其特征在于所述的复位响应判断装置，如果不建立复位响应文件，则将复位响应设置为芯片的序列号，然后执行发送装置。

22、根据权利要求 18 所述的集成电路卡的数据操作装置，其特征在于所述的协议判断装置，如果通讯协议为 T=1，则执行如下装置：

接收地址装置，接收节点地址；

第一接收判断装置，判断接收是否正确；

第一超时判断装置，判断是否超时；

接收控制字节装置，接收协议控制字节；

第二接收判断装置，判断接收是否正确；

第二超时判断装置，判断是否超时；

接收长度装置，接收数据域的长度；

第三接收判断装置，判断接收是否正确；

第三超时判断装置，判断是否超时；

接收数据装置，接收数据；

接收校验装置，接收校验和；

校验判断装置，判断校验和是否正确；

然后返回指令判断装置；

23、根据权利要求 22 所述的集成电路卡的数据操作装置，其特征在于所述的第一接收判断装置，如果接收不正确，则置错误标志，然后返回接收控制装置。

24、根据权利要求 22 所述的集成电路卡的数据操作装置，其特征在于所述的第二接收判断装置，如果接收不正确，则置错误标志，然后返回接收长度装置。

25、根据权利要求 22 所述的集成电路卡的数据操作装置，其特征在于所述的第三接收判断装置，如果接收不正确，则置错误标志，然后返回接收数据装置。

26、根据权利要求 22 所述的集成电路卡的数据操作装置，其特征在于所述的校验判断装置，如果校验和不正确，则置错误标志，然后返回接收指令判断装置。

27、根据权利要求 18 所述的集成电路卡的数据操作装置，其特征在于所述的指令判断装置，如果不是特殊指令，则执行如下装置：

查找装置，查找命令类型表；

查找判断装置，判断查找是否成功；

取命令表装置，根据程序控制字节判断命令表的存放位置，相应的取 EEPROM 或 ROM 中的命令表；

查找命令判断装置，判断查找命令是否成功；

命令类型判断装置，判断命令类型是否成功；

命令处理装置，如果是 T=0 的协议，则返回指令代码，并判断是否接收数据，是则接收数据，否则直接执行命令判断装置；

命令判断装置，判断是否满足执行条件；

执行命令装置，执行相应命令；

返回复位响应判断装置。

28、根据权利要求 27 所述的集成电路卡的数据操作装置，其特

征在于所述的查找判断装置，如果查找不成功，则置错误代码，并返回复位响应判断装置。

29、根据权利要求 27 所述的集成电路卡的数据操作装置，其特征在于所述的查找命令判断装置，如果查找不成功，则置错误代码，并返回复位响应判断装置。

30、根据权利要求 27 所述的集成电路卡的数据操作装置，其所述的命令类型判断装置，如果不成功，则置错误代码，并返回复位响应判断装置。

31、根据权利要求 18 所述的集成电路卡的数据操作装置，其文件结构包括：

主控文件（Master,MF），主控文件是整个文件系统的根，可看作根目录，每个集成电路卡有且只有一个主控文件，它是在卡的个人化过程中首先被建立起来的，在卡的整个生命周期内一直存在并保持有效，可存储卡的公共住处并为各种应用服务；由个人化建立起来的主控文件包括文件控制参数以及文件安全属性等信息；在物理上，主控文件占有存储空间包括 MF 文件头的大小以及 MF 所管理的 EF 和 DF 的存储空间；

专用文件(Dedicated File,DF)，在 MF 下针对不同的应用建立起来的一种文件，是位于 MF 之下的含有 EF 的一种文件结构（可看作文件目录），它存储了某个应用的全部数据以及与应用操作相关的安全数据；

DF 由创立文件命令建立，它的大小在建立后没有被确定，随其下建文件的空间大小而改变，对 DF 的建立操作由 MF 的安全属性控

制；

在 DF 下面不可再建立了 DF，只能建立 EF；

为了保证各个 DF 的相互独立，只能从文件系统的 MF 层次选择一个 DF，对 DF 下的数据进行的操作由各当前进系统的安全状态控制；

基本文件（Elementary File,EF），基本文件存储了各种应用的数据和管理信息，它存在于 MF 或 DF 下；

整个文件系统的空间在 MF、DF 和 EF 建立时被分配和确定，以后在物理上不会发生变化，当访问 EF 时，必须先选择相应的 MF 或 DF；

可以从文件系统的任何位置选择 MF。

32、根据权利要求 31 所述的集成电路卡的数据操作方法，其所述的基本文件从存储内容上分为两类：安全基本文件和工作基本文件；

安全基本文件（Secret Elementary File,SEF）的内容包括用于用记识别和与加密有关的保密数据（个人识别码、密钥等），卡将利用这些数据进行安全管理，SEF 要在 MF 或 DF 建立后，才能建立，安全基本文件的内容不可被读出，但可使用专门的方法来写入或修改，在 MF 和每个 DF 下只能建立 1 个安全基本文件；

工作基本文件（Working Elementary File,WEF）包含了应用的实际数据，其内容不被卡解释，在符合 WEF 的读、修改安全属性时，可对其内容进行读取、修改，工作文件的个数和大小受到 MF 或 DF 所拥有空间的限制。

33、根据权利要求 31 所述的集成电路卡的数据操作方法，其所述的基本文件的结构包括：

二进制结构，二进制文件为一个数据单元序列，数据以字节为单位进行读写，其中的数据结构则由应用解释；

线性定长记录文件结构，这种结构以固定的长度来处理每条记录；通过逻辑上连续的记录号，可访问这类记录，记录号的范围是 1 至 254，记录长度最长为 249 字节；每次访问只对一条记录进行操作，而且必须严格遵守记录长度的规定，

线性这长记录文件结构，在这类结构中，每条记录的垂度可以各不相同；仍然是以记录号为访问各条记录。在读记录时，操作与线性定长记录的相同，写记录时可以与原记录长度不同，但不能超过原记录长度；添加记录时，记录的长度不能超过最大记录长度（249 字节）的规定；

循环定长记录文件结构，一类特殊的定长记录文件结构；在逻辑上，这类文件可看作一个环形记录队列，记录按照先进先出的原则存储；添加记录时，最新一次写入的记录的记录为 1，上一次写入的记录的记录号为 2，依次类推；记录的个数与预留的记录的记录空间大小以及记录的长度相关，记录个数=记录空间大小整除记录长度；

此外还有一些只能特殊使用的文件类型，如 ATR、钱包文件、存折文件、密钥文件等，但其文件结构也不超出以上四种文件的类型。

34、根据权利要求 31 所述的集成电路卡的数据操作方法，其所

述的文件组织如下：

主控文件含有但不限于下列数据：文件名，文件标识符，所属文件的管理权限，所属专用文件的链表，所属基本文件的链表，卡片的可用空间地址，卡片的状态；

专用文件含有不限于下列数据：文件名，文件标识符，所属文件的管理权限，所属专用文件的链表，下一个专用文件的链表，所属基本文件的链表，专用文件的状态；

基本文件含有但不限于下列数据：文件名，文件标识符，基本文件的安全条件，基本文件的状态，文件长度或记录数和记录长度，记录指针；

各文件间与指针的形式实现相互间的联系。

集成电路卡的数据操作方法及装置

技术领域

本发明涉及一种数据操作方法及装置，特别涉及一种集成电路卡的数据操作方法及装置。

背景技术

集成电路卡从接口方式上分，可以分为接触式集成电路卡、非接触式集成电路及复合卡。从器件技术上分，可分为非加密存储卡、加密存储卡。非加密卡没有安全性，可以任意改写出卡内的数据，加密存储卡在普通存储卡的基础上加了逻辑加密电路，成了加密存储卡。逻辑加密存储卡由于采用密码控制逻辑来控制对 EEPROM 的访问和改写，在使用之前需要校验密码才可以进行写操作，所以对芯片本身来说是安全的，但在应用上是不安全的。它有如下不安全性因素：

1、密码在线路上是明文传输的，易被截取；

2、对于系统商来说，密码及加密算法都透明的；

3、逻辑加密卡是无法认证应用是否合法的。假设有人伪造了银行 ATM 机，你无法知道它的合法性，当您插入信用卡，输入密码的时候，信用卡的密码就被截获了。再如在互联网上购物，如果用逻辑加密卡，购物者同样无法确定网上商店的合法性。

正是由于逻辑加密卡使用上的不安全因素，促使人们考虑发展带操作系统的集成电路卡，可以做到对人、对卡、对系统的三方的合法性认证。

发明内容

本发明的目的是提供一种集成电路卡的数据操作方法及装置，应用在集成电路卡上，可做到对人、对卡、对系统的三方的合法性认证。

一种集成电路卡的数据操作方法，包括以下步骤：

初始化步骤，初始化集成电路卡的工作区，集成电路卡的工作区主要用于临时工作数据的暂存；

计算步骤，计算存储器中的系统控制信息的完整性，存储器主要存储应用程序和数据，系统控制信息包括但不限于起始地址、终止地址、卡片状态、操作系统的版本号、程序控制字节、CRC 校验；

完整性判断步骤，判断系统控制信息的完整性；

程序控制步骤，对系统控制信息中的程序控制字节进行判断，决定或者执行存储器中的应用程序，或者准备相应协议的复位信息；

复位响应判断步骤，判断是否建立复位响应文件；

取响应数据步骤，取复位响应文件中的复位响应数据；

发送步骤，发送复位响应数据；

恢复步骤，恢复备份数据；

协议判断步骤，判断通讯协议是否为 T=0；

传输步骤，卡接受由接口设备传输过来的命令头，命令头包括

但不限于指令类型、指令代码、参数；

指令判断步骤，判断是否特殊指令；

状态判断步骤，判断卡片状态是否正确；

清标志步骤，清工作标志；

协议处理步骤，如果是 T=0 协议，则返回指令代码，发送应答数据；如果是 T=1 协议，则延时，设置节点地址的值和设置协议控制字节的值，发送应答数据；

协议设置步骤，判断通讯协议标志，设置通讯协议类型；

返回复位响应判断步骤。

一种集成电路卡的数据操作装置，包括以下装置：

初始化装置，初始化集成电路卡的工作区，集成电路卡的工作区主要用于临时工作数据的暂存；

计算装置，计算存储器中的系统控制信息的完整性，存储器主要存储应用程序和数据，系统控制信息包括但不限于起始地址、终止地址、卡片状态、操作系统的版本号、程序控制字节、CRC 校验；

完整性判断装置，判断系统控制信息的完整性；

程序控制装置，对系统控制信息中的程序控制字节进行判断，决定或者执行存储器中的应用程序，或者准备相应协议的复位信息；

复位响应判断装置，判断是否建立复位响应文件；

取响应数据装置，取复位响应文件中的复位响应数据；

发送装置，发送复位响应数据；

恢复装置，恢复备份数据；

协议判断装置，判断通讯协议是否为 T=0；

传输装置，卡接受由接口设备传输过来的命令头，命令头包括但不限于指令类型、指令代码、参数；

指令判断装置，判断是否特殊指令；

状态判断装置，判断卡片状态是否正确；

清标志装置，清工作标志；

协议处理装置，如果是 T=0 协议，则返回指令代码，发送应答数据；如果是 T=1 协议，则延时，设置节点地址的值和设置协议控制字节的值，发送应答数据；

协议设置装置，判断通讯协议标志，设置通讯协议类型；

返回复位响应判断装置。

本发明所述的数据操作方法及装置应用于集成电路卡，保证了卡的安全性。

附图说明

图 1 至 5 为本发明所述的数据操作方法的流程图；

图 6 为本发明所述的数据操作方法的文件结构图；

图 7 为本发明所述的集成电路卡的硬件结构图。

具体实施方式

如图 7 所示，EEPROM 用于存放用户数据；ROM 中用于存放集成电路卡的数据操作系统，而 RAM 区中用于存放数据操作时的中间变量。

如图 1 至 7 所示，一种集成电路卡的数据操作方法，包括以下

步骤：

初始化步骤，初始化集成电路卡的工作区，集成电路卡的工作区主要用于临时工作数据的暂存；

计算步骤，计算存储器中的系统控制信息的完整性，存储器主要存储应用程序和数据，系统控制信息包括但不限于起始地址、终止地址、卡片状态、操作系统的版本号、程序控制字节、CRC 校验；

完整性判断步骤，判断系统控制信息的完整性；

程序控制步骤，对系统控制信息中的程序控制字节进行判断，决定或者执行存储器中的应用程序，或者准备相应协议的复位信息；

复位响应判断步骤，判断是否建立复位响应文件；

取响应数据步骤，取复位响应文件中的复位响应数据；

发送步骤，发送复位响应数据；

恢复步骤，恢复备份数据；

协议判断步骤，判断通讯协议是否为 T=0；

传输步骤，卡接受由接口设备传输过来的命令头，命令头包括但不限于指令类型、指令代码、参数；

指令判断步骤，判断是否特殊指令；

状态判断步骤，判断卡片状态是否正确；

清标志步骤，清工作标志；

协议处理步骤，如果是 T=0 协议，则返回指令代码，发送应答数据；如果是 T=1 协议，则延时，设置节点地址的值和设置协议控制字节的值，发送应答数据；

协议设置步骤，判断通讯协议标志，设置通讯协议类型；

返回复位响应判断步骤。

所述的完整性判断步骤，如果不完整，则锁卡并更新存储器中的系统控制信息，然后执行程序控制步骤；

所述的程序控制步骤中执行存储器中的应用程序一般为集成电路卡使用者自己设定的加密程序。

所述的复位响应判断步骤，如果不建立复位响应文件，则将复位响应设置为芯片的序列号，然后执行发送步骤。

所述的协议判断步骤，如果通讯协议为 T=1，则执行如下步骤：

接收地址步骤，接收节点地址；

第一接收判断步骤，判断接收是否正确；

第一超时判断步骤，判断是否超时；

接收控制字节步骤，接收协议控制字节；

第二接收判断步骤，判断接收是否正确；

第二超时判断步骤，判断是否超时；

接收长度步骤，接收数据域的长度；

第三接收判断步骤，判断接收是否正确；

第三超时判断步骤，判断是否超时；

接收数据步骤，接收数据；

接收校验步骤，接收校验和；

校验判断步骤，判断校验和是否正确；

然后返回指令判断步骤；

所述的第一接收判断步骤，如果接收不正确，则置错误标志，然后返回接收控制步骤。

所述的第二接收判断步骤，如果接收不正确，则置错误标志，然后返回接收长度步骤。

所述的第三接收判断步骤，如果接收不正确，则置错误标志，然后返回接收数据步骤。

所述的校验判断步骤，如果校验和不正确，则置错误标志，然后返回接收指令判断步骤。

所述的指令判断步骤，如果不是特殊指令，则执行如下步骤：

查找步骤，查找命令类型表；

查找判断步骤，判断查找是否成功；

取命令表步骤，根据程序控制字节判断命令表的存放位置，相应的取 EEPROM 或 ROM 中的命令表；

查找命令判断步骤，判断查找命令是否成功；

命令类型判断步骤，判断命令类型是否成功；

命令处理步骤，如果是 T=0 的协议，则返回指令代码，并判断是否接收数据，是则接收数据，否则直接执行命令判断步骤；

命令判断步骤，判断是否满足执行条件；

执行命令步骤，执行相应命令；

返回复位响应判断步骤。

所述的查找判断步骤，如果查找不成功，则置错误代码，并返回复位响应判断步骤。

所述的查找命令判断步骤，如果查找不成功，则置错误代码，并返回复位响应判断步骤。

所述的命令类型判断步骤，如果不成功，则置错误代码，并返

回复位响应判断步骤。

一种集成电路卡的数据操作装置，包括以下装置：

初始化装置，初始化集成电路卡的工作区，集成电路卡的工作区主要用于临时工作数据的暂存；

计算装置，计算存储器中的系统控制信息的完整性，存储器主要存储应用程序和数据，系统控制信息包括但不限于起始地址、终止地址、卡片状态、操作系统的版本号、程序控制字节、CRC 校验；

完整性判断装置，判断系统控制信息的完整性；

程序控制装置，对系统控制信息中的程序控制字节进行判断，决定或者执行存储器中的应用程序，或者准备相应协议的复位信息；

复位响应判断装置，判断是否建立复位响应文件；

取响应数据装置，取复位响应文件中的复位响应数据；

发送装置，发送复位响应数据；

恢复装置，恢复备份数据；

协议判断装置，判断通讯协议是否为 T=0；

传输装置，卡接受由接口设备传输过来的命令头，命令头包括但不限于指令类型、指令代码、参数；

指令判断装置，判断是否特殊指令；

状态判断装置，判断卡片状态是否正确；

清标志装置，清工作标志；

协议处理装置，如果是 T=0 协议，则返回指令代码，发送应答数据；如果是 T=1 协议，则延时，设置节点地址的值和设置协议控制字节的值，发送应答数据；

协议设置装置，判断通讯协议标志，设置通讯协议类型；

返回复位响应判断装置。

所述的完整性判断装置，如果不完整，则锁卡并更新存储器中的系统控制信息，然后执行程序控制装置；

所述的程序控制装置中执行存储器中的应用程序一般为集成电路卡使用者自己设定的加密程序。

所述的复位响应判断装置，如果不建立复位响应文件，则将复位响应设置为芯片的序列号，然后执行发送装置。

所述的协议判断装置，如果通讯协议为 T=1，则执行如下装置：

接收地址装置，接收节点地址；

第一接收判断装置，判断接收是否正确；

第一超时判断装置，判断是否超时；

接收控制字节装置，接收协议控制字节；

第二接收判断装置，判断接收是否正确；

第二超时判断装置，判断是否超时；

接收长度装置，接收数据域的长度；

第三接收判断装置，判断接收是否正确；

第三超时判断装置，判断是否超时；

接收数据装置，接收数据；

接收校验装置，接收校验和；

校验判断装置，判断校验和是否正确；

然后返回指令判断装置；

所述的第一接收判断装置，如果接收不正确，则置错误标志，

然后返回接收控制装置。

所述的第二接收判断装置，如果接收不正确，则置错误标志，然后返回接收长度装置。

所述的第三接收判断装置，如果接收不正确，则置错误标志，然后返回接收数据装置。

所述的校验判断装置，如果校验和不正确，则置错误标志，然后返回接收指令判断装置。

所述的指令判断装置，如果不是特殊指令，则执行如下装置：

查找装置，查找命令类型表；

查找判断装置，判断查找是否成功；

取命令表装置，根据程序控制字节判断命令表的存放位置，相应的取 EEPROM 或 ROM 中的命令表；

查找命令判断装置，判断查找命令是否成功；

命令类型判断装置，判断命令类型是否成功；

命令处理装置，如果是 T=0 的协议，则返回指令代码，并判断是否接收数据，是则接收数据，否则直接执行命令判断装置；

命令判断装置，判断是否满足执行条件；

执行命令装置，执行相应命令；

返回复位响应判断装置。

所述的查找判断装置，如果查找不成功，则置错误代码，并返回复位响应判断装置。

所述的查找命令判断装置，如果查找不成功，则置错误代码，并返回复位响应判断装置。

所述的命令类型判断装置，如果不成功，则置错误代码，并返回复位响应判断装置。

上述的数据操作方法及装置应用于集成电路卡是以文件方式来管理的，如图6所示，文件结构包括：

主控文件（Master,MF），主控文件是整个文件系统的根，可看作根目录，每个集成电路卡有且只有一个主控文件，它是在卡的个人化过程中首先被建立起来的，在卡的整个生命周期内一直存在并保持有效，可存储卡的公共住处并为各种应用服务；由个人化建立起来的主控文件包括文件控制参数以及文件安全属性等信息；在物理上，主控文件占有存储空间包括 MF 文件头的大小以及 MF 所管理的 EF 和 DF 的存储空间；

专用文件(Dedicated File,DF)，在 MF 下针对不同的应用建立起来的一种文件，是位于 MF 之下的含有 EF 的一种文件结构（可看作文件目录），它存储了某个应用的全部数据以及与应用操作相关的安全数据；

DF 由创立文件命令建立，它的大小在建立后没有被确定，随其下建文件的空间大小而改变，对 DF 的建立操作由 MF 的安全属性控制；

在 DF 下面不可再建立了 DF，只能建立 EF；

为了保证各个 DF 的相互独立，只能从文件系统的 MF 层次选择一个 DF，对 DF 下的数据进行的操作由各当前进系统的安全状态控制；

基本文件（Elementary File,EF），基本文件存储了各种应用的

数据和管理信息，它存在于 MF 或 DF 下；

整个文件系统的空间在 MF、DF 和 EF 建立时被分配和确定，以后在物理上不会发生变化，当访问 EF 时，必须先选择相应的 MF 或 DF；

可以从文件系统的任何位置选择 MF。

所述的基本文件从存储内容上分为两类：安全基本文件和工作基本文件；

安全基本文件（Secret Elementary File,SEF）的内容包括用于用记识别和与加密有关的保密数据（个人识别码、密钥等），卡将利用这些数据进行安全管理，SEF 要在 MF 或 DF 建立后，才能建立，安全基本文件的内容不可被读出，但可使用专门的方法来写入或修改，在 MF 和每个 DF 下只能建立 1 个安全基本文件；

工作基本文件（Working Elementary File,WEF）包含了应用的实际数据，其内容不被卡解释，在符合 WEF 的读、修改安全属性时，可对其内容进行读取、修改，工作文件的个数和大小受到 MF 或 DF 所拥有空间的限制。

所述的基本文件的结构包括：

二进制结构，二进制文件为一个数据单元序列，数据以字节为单位进行读写，其中的数据结构则由应用解释；

线性定长记录文件结构，这种结构以固定的长度来处理每条记录；通过逻辑上连续的记录号，可访问这类记录，记录号的范围是 1 至 254，记录长度最长为 249 字节；每次访问只对一条记录进行操作，而且必须严格遵守记录长度的规定，

线性这长记录文件结构，在这类结构中，每条记录的垂度可以各不相同；仍然是以记录号为访问各条记录。在读记录时，操作与线性定长记录的相同，写记录时可以与原记录长度不同，但不能超过原记录长度；添加记录时，记录的长度不能超过最大记录长度（249字节）的规定；

循环定长记录文件结构，一类特殊的定长记录文件结构：在逻辑上，这类文件可看作一个环形记录队列，记录按照先进先出的原则存储；添加记录时，最新一次写入的记录的记录为 1，上一次写入的记录的记录号为 2，依次类推；记录的个数与预留的记录的记录空间大小以及记录的长度相关，记录个数=记录空间大小整除记录长度；

此外还有一些只能特殊使用的文件类型，如 ATR、钱包文件、存折文件、密钥文件等，但其文件结构也不超出以上四种文件的类型。

所述的文件组织如下：

主控文件含有但不限于下列数据：文件名，文件标识符，所属文件的管理权限，所属专用文件的链表，所属基本文件的链表，卡片的可用空间地址，卡片的状态；

专用文件含有不限于下列数据：文件名，文件标识符，所属文件的管理权限，所属专用文件的链表，下一个专用文件的链表，所属基本文件的链表，专用文件的状态；

基本文件含有但不限于下列数据：文件名，文件标识符，基本文件的安全条件，基本文件的状态，文件长度或记录数和记录长度，

记录指针；

各文件间与指针的形式实现相互间的联系。

我们以一套系统的发卡的过程来解释上述的方法及装置：

1、根密钥卡及其认证卡生成流程

根密钥卡生成流程：

根密钥卡发卡流程描述：

校验生产商认证卡的 PIN：00 20 00 00 02 XX XX

用生产商认证卡鉴别每一张 IC 卡的有效性，建立 MF 文件

80 E0 00 00 0X XX XX XX XX XX XX

创建复位应答文件：给根密钥卡分配 10 字节序列号，第一字节为卡片类型，根密钥卡类型为 01，后 9 个字节为序列号，每张卡片具有唯一序列号，序列号由 00 00 00 00 00 00 00 00 01 开始分配。

80 E0 02 00 07 00 01 04 0F F0 00 0A

00 D6 00 00 0A 86 38 XX XX

MF 下创建 KEY 文件，安装和更新密钥的形式为密文+MAC，文件类型为 C5

80 E0 02 00 00 07 00 02 C5 F0 11 10 00

在生产商传输密钥的控制下装载根密钥卡的主控密钥。

使用密钥：生产商传输密钥；

加密数据：主控密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

主控密钥由特殊算法生成。

在主控密钥的控制下装载根密钥。

使用密钥：主控密钥；

加密数据：根密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

根密钥由特殊算法生成。

在主控密钥的控制下装载外部认证密钥。

使用密钥：主控密钥；

加密数据：外部认证密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

外部认证密钥由特殊算法生成。

在主控密钥的控制下装载应用维护密钥。

使用密钥：主控密钥；

加密数据：应用维护密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

应用维护密钥由特殊算法生成。

在主控密钥的控制下装载传输密钥。

使用密钥：主控密钥；

加密数据：传输密钥的密钥信；

MAC 初始值：4 字节随机数+ 00 00 00 00。

在 MF 下创建二进制文件 0003，文件类型为 00，并将根密钥卡的发卡信息写入保存。

80 E0 02 00 07 00 03 00 11 11 00 20

00 D6 00 00 0X XXXXXXXXXX

MF 创建结束。

80 E0 00 01 02 3F 00

根密钥认证卡生成流程：

根密钥认证卡发卡流程描述：

用生产商认证卡鉴别每一张 IC 卡的有效性，建立 MF 文件

80 E0 00 00 0X XX XX XX XX XX XX

创建复位应答文件：给根密钥认证卡分配 10 字节序列号，第一字节为卡片类型，根密钥认证卡类型为 02，后 9 个字节为序列号，每张卡片具有唯一序列号，序列号由 00 00 00 00 00 00 00 00 01 开始分配。

80 E0 02 00 07 00 01 04 0F F0 00 0A

00 D6 00 00 0A 86 38 XX XX

MF 下创建 KEY 文件，安装和更新密钥的形式为密文+MAC，文件类型为 C5

80 E0 02 00 00 07 00 02 C5 F0 11 10 00

在生产商传输密钥的控制下装载根密钥认证卡的主控密钥。

使用密钥：生产商传输密钥；

加密数据：主控密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

在主控密钥的控制下装载 PIN、SPIN（由系统安全管理员输入）。

使用密钥：主控密钥 ；

加密数据：PIN、SPIN 的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

在主控密钥的控制下装载内部认证密钥。

使用密钥：主控密钥 ；

加密数据：内部认证密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

内部认证密钥值与根密钥卡外部认证密钥值相同。

在主控密钥的控制下装载 MAC 加密密钥。

使用密钥：主控密钥 ；

加密数据：MAC 加密密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

MAC 加密密钥值与根密钥卡传输密钥值相同。

MF 创建结束：80 E0 00 01 02 3F 00

2、主密钥卡及其认证卡生成流程

主密钥卡生成流程：

主密钥卡发卡流程描述：

校验生产商认证卡的 PIN：00 20 00 00 02 XX XX

从生产商认证卡读取传输代码

根密钥卡与根密钥认证卡相互认证

根密钥认证卡：校验 PIN 00 20 00 00 02 XXXX

根密钥卡：取随机数 00 84 00 00 04

根密钥认证卡：内部认证 00 88 00 00 08 随机数 + 00 00 00 00

根密钥卡：外部认证 00 82 00 02 08 XXXXXXX

替换根密钥卡的传输密钥

根密钥卡：取随机数 00 84 00 00 04

根密钥认证卡：DES 初始化 80 1A 08 01 00

DES 计算 80 FA 00 00 18 XXXXXXXXXX

DES 初始化 80 1A 08 01 00

MAC 计算 80 FA 00 02 0X XXXXXXXXX

根密钥卡：修改密钥 84 D4 0E 01 0X XXXXXXXX

替换根密钥认证卡的 MAC 加密密钥

根密钥认证卡：取随机数 00 84 00 00 04

根密钥认证卡：DES 初始化 80 1A 08 01 00

DES 计算 80 FA 00 00 18 XXXXXXXXX

DES 初始化 80 1A 08 01 00

MAC 计算 80 FA 00 02 0X XXXXXXXXXX

根密钥认证卡：修改密钥 84 D4 08 01 0X XXXXXXXXX

建立 MF 文件，鉴别每一张 IC 卡的有效性

80 E0 00 00 0X XX XX XX XX XX XX

创建复位应答文件：给主密钥卡分配 10 字节序列号，第一字节为卡片类型，主密钥卡类型为 03，后 9 个字节为序列号，每张卡片具有唯一序列号，序列号由 00 00 00 00 00 00 00 00 01 开始分配。

80 E0 02 00 07 00 01 04 0F F0 00 0A

00 D6 00 00 0A 86 38 XX XX

MF 下创建 KEY 文件，安装和更新密钥的形式为密文+MAC，文件类型为 C5

80 E0 02 00 00 07 00 02 C5 F0 11 10 00

在生产商传输密钥的控制下装载主密钥卡的主控密钥。

使用密钥：生产商传输密钥；

加密数据：主控密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

主控密钥由特殊算法生成。

通过根密钥对城市 ID 分散得到主密钥卡的主密钥，并在主控密钥的控制下装入 KEY 文件。

密钥导出使用 OUT KEY 命令，导出方式为密文分散导出方式（P1=21），控制密钥为根密钥卡中的传输密钥。

在主控密钥的控制下装载外部认证密钥。

使用密钥：主控密钥；

加密数据：外部认证密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

外部认证密钥由特殊算法生成。

在主控密钥的控制下装载应用维护密钥。

使用密钥：主控密钥；

加密数据：应用维护密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

应用维护密钥由特殊算法生成。

在主控密钥的控制下装载传输密钥。

使用密钥：主控密钥；

加密数据：传输密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

在 MF 下创建二进制文件 0003，文件类型为 00，并将主密钥卡的发卡信息写入保存。

80 E0 02 00 07 00 03 00 11 11 00 20

00 D6 00 00 0X XXXXXXXXXX

MF 创建结束。

80 E0 00 01 02 3F 00

主密钥认证卡生成流程：

主密钥认证卡发卡流程描述：

用生产商认证卡鉴别每一张 IC 卡的有效性，建立 MF 文件

80 E0 00 00 0X XX XX XX XX XX XX

创建复位应答文件：给主密钥认证卡分配 10 字节序列号，第字节为卡片类型，主密钥认证卡类型为 04，后 9 个字节为序列号，每张卡片具有唯一序列号，序列号由 00 00 00 00 00 00 00 00 01 开始分配。

80 E0 02 00 07 00 01 04 0F F0 00 0A

00 D6 00 00 0A 86 38 XX XX

MF 下创建 KEY 文件，安装和更新密钥的形式为密文+MAC，文 件类型为 C5

80 E0 02 00 00 07 00 02 C5 F0 11 10 00

在生产商传输密钥的控制下装载主密钥认证卡的主控密钥。

使用密钥：生产商传输密钥；

加密数据：主控密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

在主控密钥的控制下装载 PIN、SPIN（由系统安全管理员输入）。

使用密钥：主控密钥 ；

加密数据：PIN、SPIN 的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

在主控密钥的控制下装载内部认证密钥。

使用密钥：主控密钥 ；

加密数据：内部认证密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

内部认证密钥值与根密钥卡外部认证密钥值相同。

在主控密钥的控制下装载 MAC 加密密钥。

使用密钥：主控密钥 ；

加密数据：MAC 加密密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

MAC 加密密钥值与主密钥卡传输密钥值相同。

MF 创建结束：80 E0 00 01 02 3F 00。

3、PSAM 卡生成流程

PSAM 卡生成流程：

PSAM 卡发卡流程描述：

校验生产商认证卡的 PIN：00 20 00 00 02 XX XX

生产商认证卡读取传输代码

根密钥卡与根密钥认证卡相互认证。

根密钥认证卡：校验 PIN 00 20 00 00 02 XXXX

根密钥卡：取随机数 00 84 00 00 04

根密钥认证卡：内部认证 00 88 00 00 08 随机数 + 00 00 00 00

根密钥卡：外部认证 00 82 00 02 08 XXXXXXX

替换根密钥卡的传输密钥。

根密钥卡：取随机数 00 84 00 00 04

根密钥认证卡：DES 初始化 80 1A 08 01 00

DES 计算 80 FA 00 00 18 XXXXXXXXXX

DES 初始化 80 1A 08 01 00

MAC 计算 80 FA 00 02 0X XXXXXXXXXX

根密钥卡：修改密钥 84 D4 0E 01 0X XXXXXXXXX

替换根密钥认证卡的 MAC 加密密钥。

根密钥认证卡：取随机数 00 84 00 00 04

根密钥认证卡：DES 初始化 80 1A 08 01 00

DES 计算 80 FA 00 00 18 XXXXXXXXXX

DES 初始化 80 1A 08 01 00

MAC 计算 80 FA 00 02 0X XXXXXXXXXX

根密钥认证卡：修改密钥 84 D4 08 01 0X XXXXXXXXX

建立 MF 文件，鉴别每一张 IC 卡的有效性。

80 E0 00 00 0X XX XX XX XX XX XX

创建复位应答文件：给 PSAM 卡分配 10 字节序列号，每张卡片具有唯一序列号，序列号由 00 00 00 00 00 00 00 00 00 01 开始分配。

80 E0 02 00 07 00 01 04 0F F0 00 0A

00 D6 00 00 0A XX XX XX XX

MF 下创建 KEY 文件，安装和更新密钥的形式为密文+MAC，文件类型为 C5

80 E0 02 00 00 07 00 02 C5 F0 0F 10 00

在生产商传输密钥的控制下装载主密钥卡的主控密钥。

使用密钥：生产商传输密钥；

加密数据：主控密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

主控密钥由特殊算法生成。

在主控密钥的控制下装载维护密钥。

使用密钥：主控密钥；

加密数据：维护密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

维护密钥由特殊算法生成。

在 MF 下创建卡片公共信息文件，写入卡片公共信息。

80 E0 02 00 07 00 15 00 0F 0F 00 0E

00 D6 00 00 0X XXXXXXXXXXX

在 MF 下创建终端信息文件，写入终端机编号。

80 E0 02 00 07 00 16 00 0F 0F 00 06

00 D6 00 00 0X XXXXXXXXXXX

在 MF 下创建 DIR 文件，写入应用名称。

80 E0 02 00 07 00 03 03 0F 0F 00 C8

00 E2 00 00 0X XXXXXXXXXXX

创建 ADF 文件：80 E0 01 00 0X XXXXXXXXXXX

创建 ADF 下的 KEY 文件：80 E0 02 00 07 00 01 C5 0F 11 10 00

在主控密钥的控制下装载应用主控密钥。

使用密钥：主控密钥；

加密数据：应用主控密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

应用主控密钥由特殊算法生成。

在应用主控密钥的控制下装载应用维护密钥。

使用密钥：应用主控密钥；

加密数据：应用维护密钥的密钥信息；

MAC 初始值：4 字节随机数+ 00 00 00 00。

应用维护密钥由特殊算法生成。

通过根密钥卡直接导入根密钥。

密钥导出使用 OUT KEY 命令，导出方式为密文直接导出方式（P1=61），控制密钥为根密钥卡中的传输密钥。

创建应用公共信息文件，写入应用公共信息。

80 E0 02 00 07 00 17 00 0F 0F 00 19

00 D6 00 00 0X XXXXXXXXXX

创建终端应用交易序号文件。

80 E0 02 00 07 00 18 00 0F 0F 00 04

DF 创建结束。

80 E0 01 01 02 3F 00

MF 创建结束。

80 E0 00 01 02 3F 00

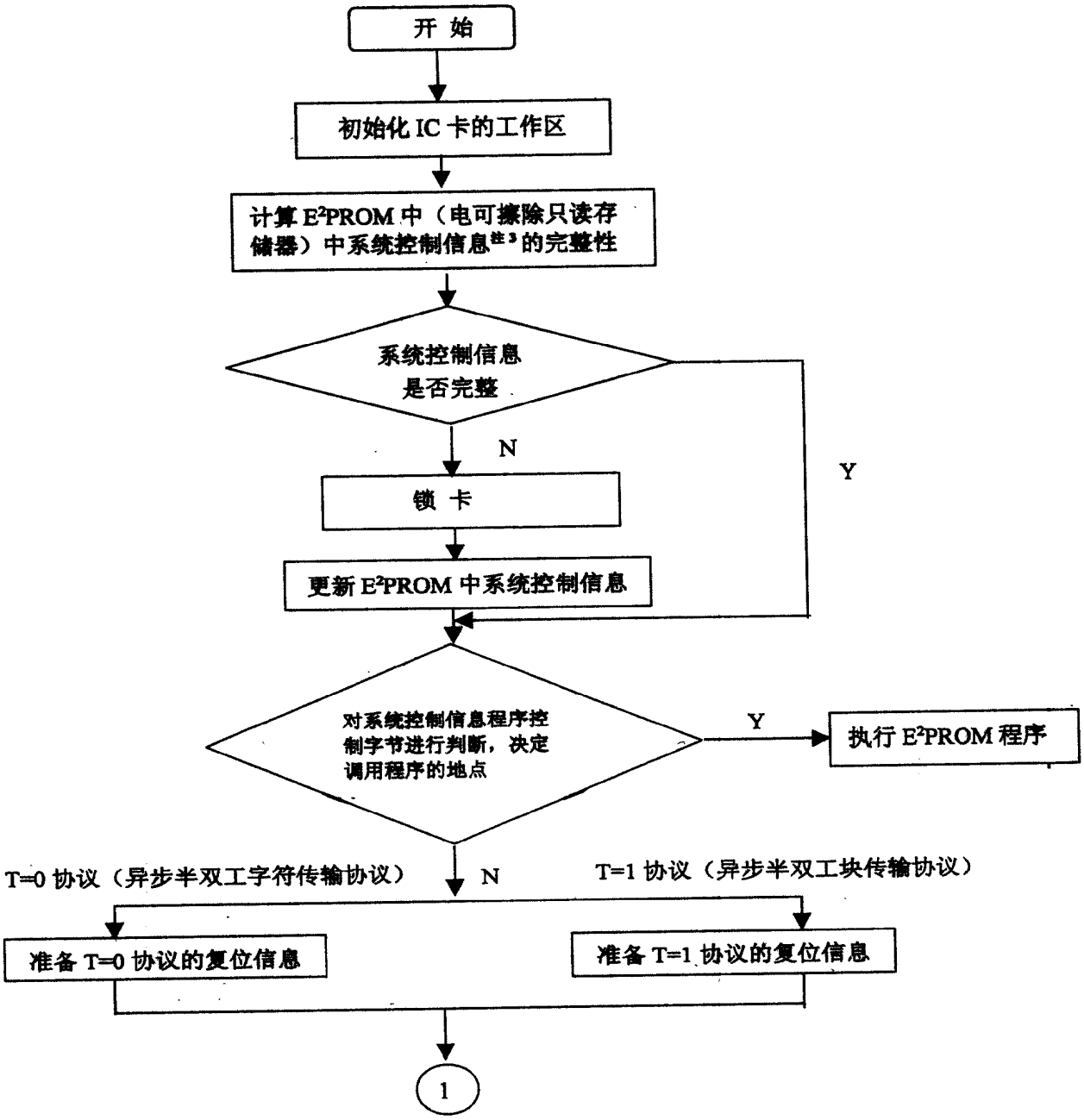
开 始
初始化 IC 卡的工作区
计算 E²PROM 中（电可擦除只读存储器）中系统控制信息注3的完整性
系统控制信息是否完整
N
Y
锁 卡
更新 E²PROM 中系统控制信息
对系统控制信息程序控制字节进行判断，决定调用程序的地点
Y
执行 E²PROM 程序
T=0 协议（异步半双工字符传输协议）
N
T=1 协议（异步半双工块传输协议）
准备 T=0 协议的复位信息
准备 T=1 协议的复位信息
1

图 1

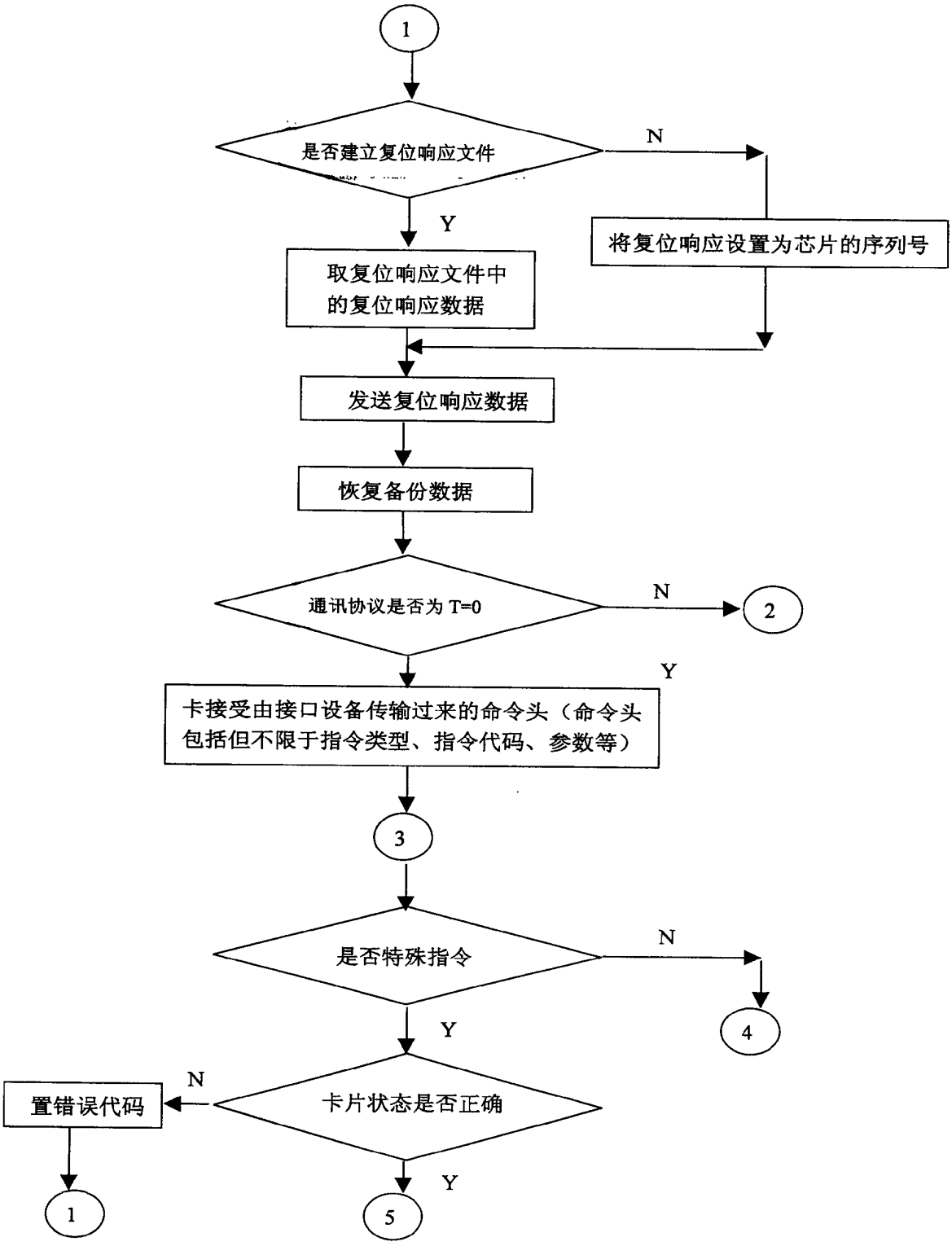
1
是否建立复位响应文件
N
Y
将复位响应设置为芯片的序列号
取复位响应文件中
的复位响应数据
发送复位响应数据
恢复备份数据
通讯协议是否为 T=0
N
2
Y
卡接受由接口设备传输过来的命令头（命令头
包括但不限于指令类型、指令代码、参数等）
3
是否特殊指令
N
4
Y
卡片状态是否正确
N
置错误代码
1
Y
5

图 2

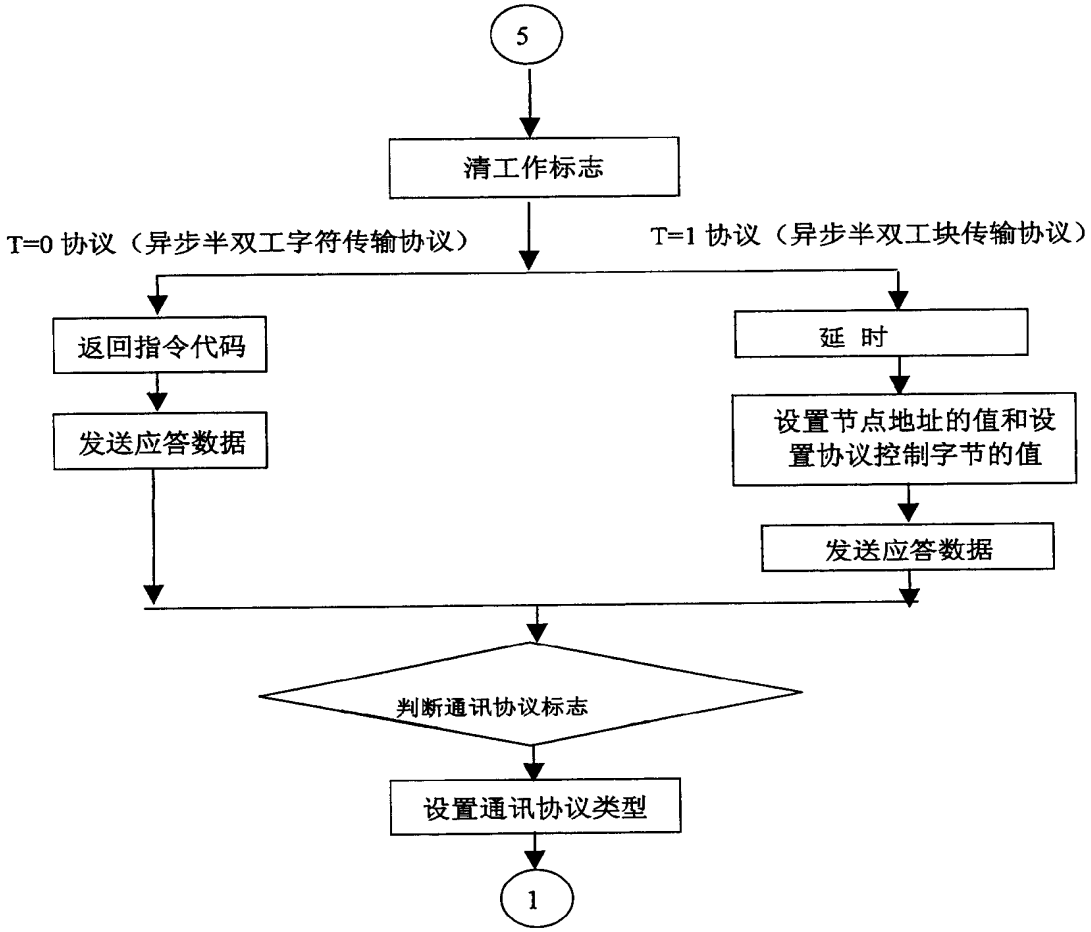
5
清工作标志
T=0 协议（异步半双工字符传输协议）
T=1 协议（异步半双工块传输协议）
返回指令代码
发送应答数据
延 时
设置节点地址的值和设置协议控制字节的值
发送应答数据
判断通讯协议标志
设置通讯协议类型
1

图 3

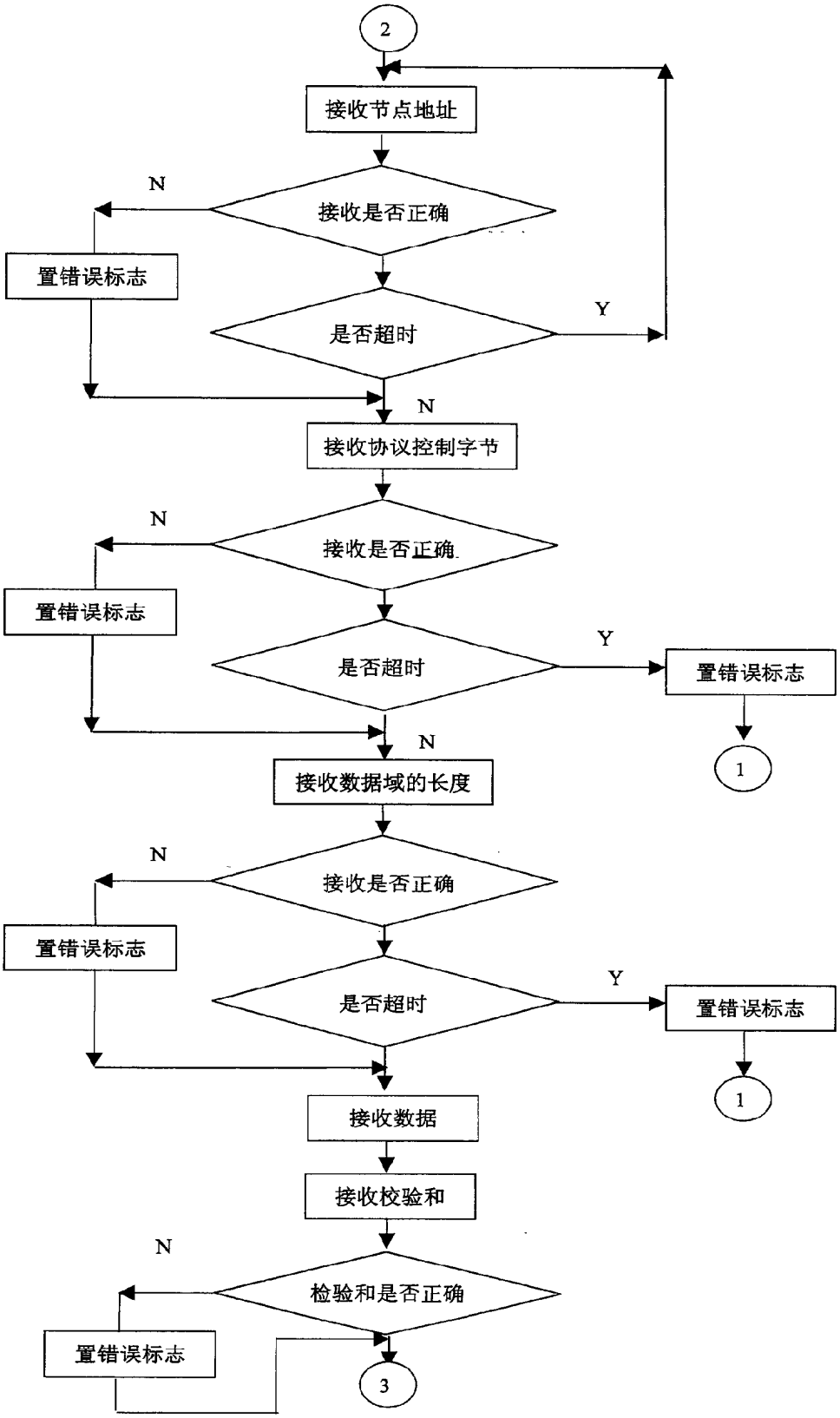
2
接收节点地址
接收是否正确
N
置错误标志
是否超时
Y
N
接收协议控制字节
接收是否正确
N
置错误标志
是否超时
Y
置错误标志
1
N
接收数据域的长度
接收是否正确
N
置错误标志
是否超时
Y
置错误标志
1
接收数据
接收校验和
检验和是否正确
N
置错误标志
3

图 4

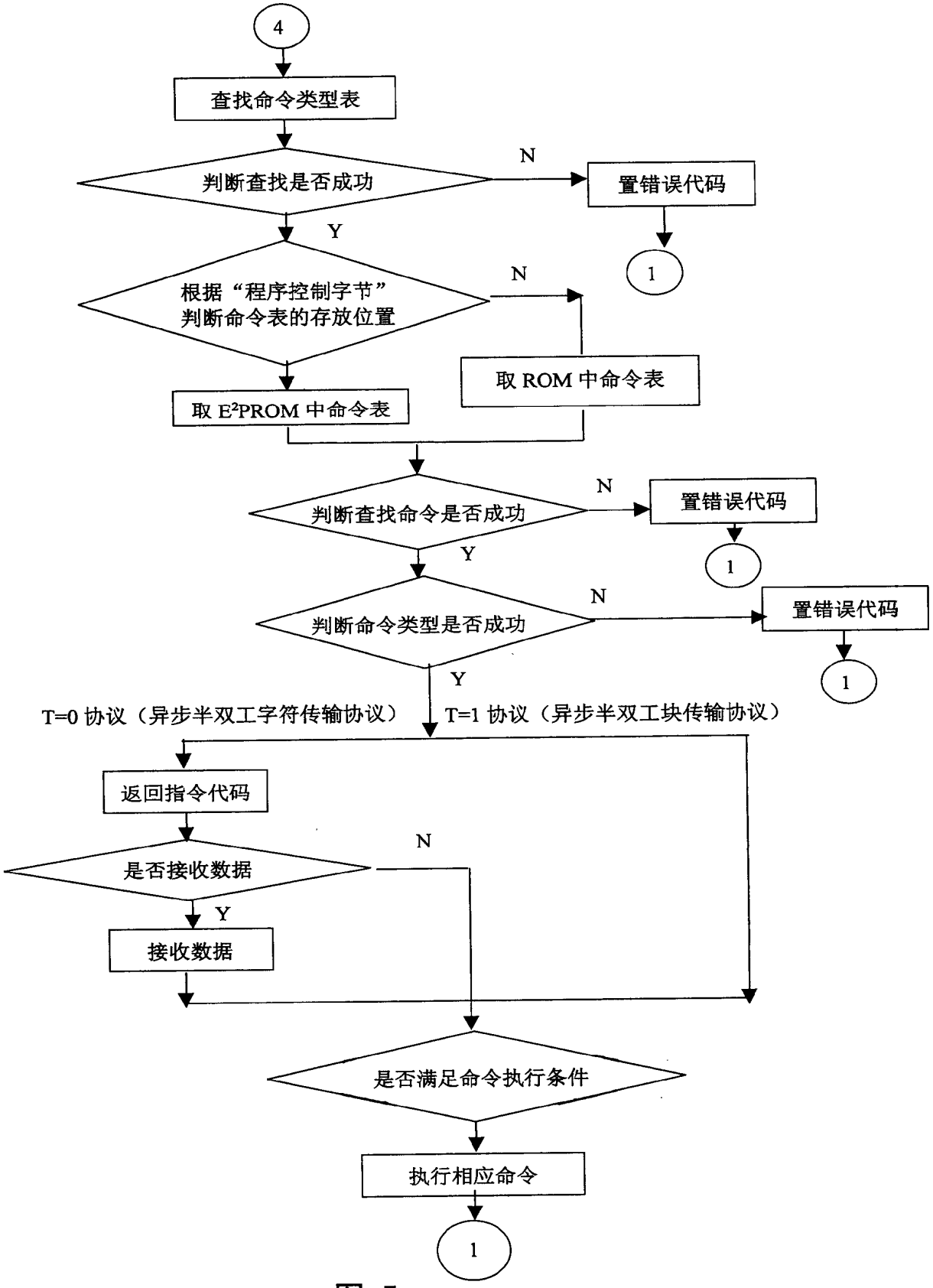
4
查找命令类型表
判断查找是否成功
N
置错误代码
1
Y
根据“程序控制字节”
判断命令表的存放位置
N
取 ROM 中命令表
取 E²PROM 中命令表
判断查找命令是否成功
N
置错误代码
1
Y
判断命令类型是否成功
N
置错误代码
1
Y
T=0 协议（异步半双工字符传输协议）
T=1 协议（异步半双工块传输协议）
返回指令代码
是否接收数据
N
Y
接收数据
是否满足命令执行条件
执行相应命令
1

图 5

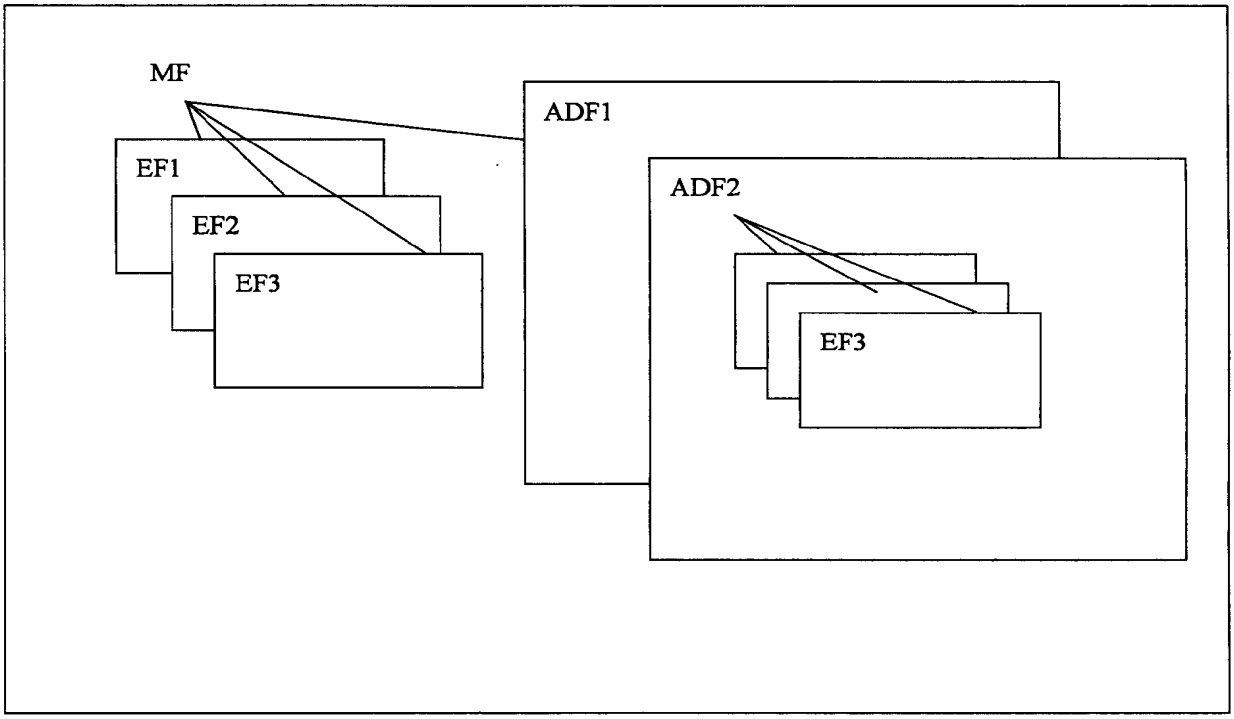

图 6

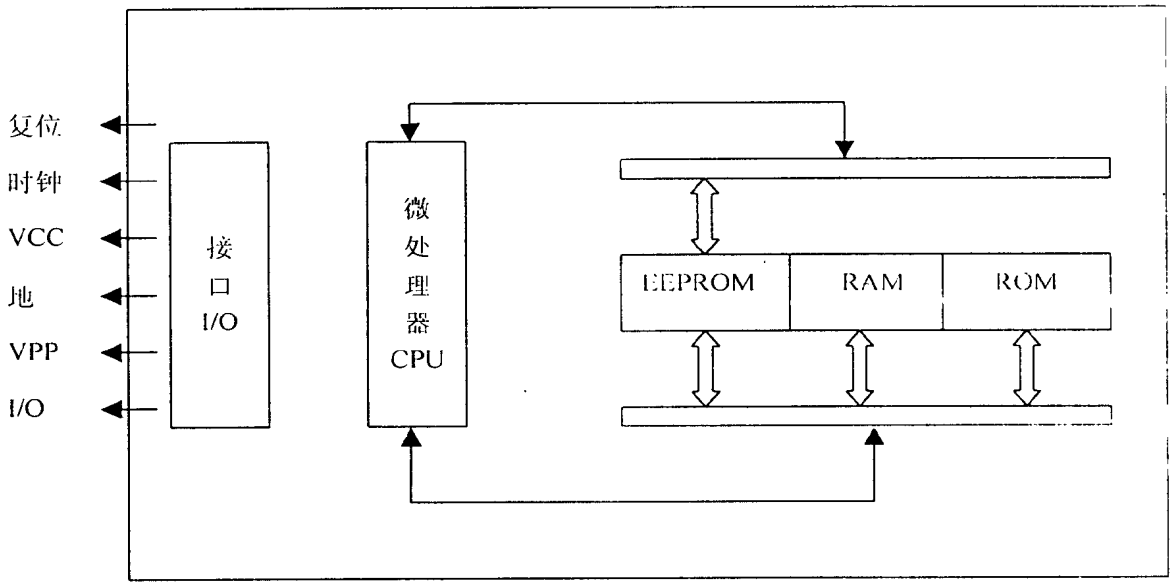

图 7